ENERGY EFFICIENT AND SECURED DATA TRANSMISSION USING IOT BASED HEALTHCARE MONITORING SYSTEM

A SYNOPSIS

Submitted by

D.BALAKRISHNAN
(Reg. No. 201807264)

in partial fulfillment for the award of the degree of

DOCTOR OF PHILOSOPHY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION

(DEEMED TO BE UNIVERSITY)

ANAND NAGAR, KRISHNANKOIL – 626 126

TAMIL NADU, INDIA

AUGUST 2024

1. INTRODUCTION

The healthcare industry is on the cusp of a revolutionary transformation fueled by the integration of Internet of Things (IoT) technology [1-3]. This advancement presents a promising landscape where patients can benefit from continuous health monitoring through wearable or implanted medical sensors, transcending geographical constraints and time limitations. These IoT devices serve as invaluable tools, capturing and transmitting essential health data to healthcare professionals, enabling instantaneous access to patients' health statuses. However, amidst these groundbreaking advancements, significant challenges loom, particularly concerning the constrained resources and computational capacities of IoT devices, leading to pressing concerns regarding energy conservation.

Efforts have been made to mitigate energy consumption in IoT networks through the implementation of clustering methods. These methods aim to conserve energy by clustering devices, thereby reducing redundant transmissions and optimizing resource usage within network nodes. Despite these initiatives, existing clustering approaches [4] encounter hurdles related to increased energy consumption, uneven distribution of network loads, and amplified end-to-end delays. These limitations necessitate further refinement and innovation in clustering methodologies to enhance energy efficiency and address these critical issues effectively.

Moreover, ensuring the sanctity and security of sensitive medical data [5] has emerged as a paramount concern in healthcare applications. The integrity, authenticity, and privacy of information transmitted through IoT devices must be safeguarded against potential vulnerabilities and threats [6]. Consequently, ongoing research endeavors focus on proposing various techniques aimed at fortifying data security measures. These techniques encompass strategies to bolster information privacy, validate message authenticity, maintain data integrity, and minimize communication overhead and computational burden.

This research work represents a concerted effort to tackle the multifaceted challenges that accompany the integration of IoT technology in healthcare. By refining clustering methodologies to optimize energy consumption and addressing security concerns through innovative data protection techniques, the goal is to create a robust

and secure ecosystem. Ultimately, these efforts aim to propel the healthcare sector towards a future where IoT-based healthcare applications offer not only seamless connectivity and real-time monitoring but also ensure the confidentiality andintegrity of patients' sensitive health information.

2. LITERATURE SURVEY

In an IoT-based healthcare system, security stands as a fundamental pillar due to the sensitive nature of patient data. Security measures are crucial to safeguard against potential cyber threats, unauthorized access, and data breaches that could compromise patient privacy and confidentiality. Ensuring robust security protocols involves implementing encryption techniques, stringent authentication mechanisms, and access controls across the interconnected devices and data transmissions. Without a secure framework, the integrity of patient information could be compromised, leading to dire consequences for individuals and healthcare providers. Therefore, enhancing security measures is essential to maintain trust, comply with data protection regulations, and safeguard sensitive healthcare data in IoT ecosystems.

Optimal data routing plays a pivotal role in the seamless and efficient transmission of healthcare information within IoT networks. Given the diverse nature of medical data generated by various devices and sensors, efficient routing algorithms are critical to ensure timely and accurate delivery of information. Analyzing and implementing optimal data routing techniques helps mitigate network congestion, reduce latency, and optimize resource utilization within the IoT infrastructure. By selecting the most efficient paths for data transmission, healthcare providers can ensure that critical information reaches its destination promptly, enhancing the quality and reliability of patient care.

Energy efficiency is a pressing concern in IoT-based healthcare systems, primarily due to the extensive deployment of interconnected devices in medical settings. Optimizing energy consumption within these devices and nodes is vital to prolong their operational life, minimize costs, and reduce the environmental impact. Efficient use of resources, smart power management, and employing energy-saving protocols contribute to sustainable operations while ensuring uninterrupted functionality of IoT devices. Proper analysis and implementation of energy-efficient strategies are essential to support the reliability and longevity of devices in healthcare

applications, preventing disruptions that could impact patient care and system performance.

Cluster Head (CH) selection is another critical aspect within IoT-based healthcare systems. Choosing appropriate CHs involves identifying nodes capable of efficiently managing data aggregation and transmission within the network. These CHs play a pivotal role in optimizing communication, data processing, and resource allocation among IoT devices. Through meticulous selection and management of CHs, healthcare systems can enhance network efficiency, reduce communication overhead, and improve overall system performance, contributing significantly to the seamless functioning of IoT- enabled healthcare environments. In order to secure the data transmission, reduce the energy efficiency, optimal data routing and optimal CH selection in IoT-enabled healthcare environment, a number of research papers are analyzed and examined.

Almalki and Soufiene [7] introduced the Efficient and Privacy-Preserving Data-Gathering technique with Authentication (EPPDA) aimed at ensuring security within IoT-HC systems. At the outset, EPPDA undertook device verification and authorization within the network to collect data from these devices. Subsequently, in order to uphold the confidentiality and reliability of the data obtained from HC devices, the system incorporated additive homomorphic encryption and homomorphic media access control. The outcomes demonstrated that the system successfully attained device authenticity, maintained data integrity and privacy, and managed communication overhead.

Prasanalakshmi et al. [8] introduced a secure method for transmitting data within an IoT-based healthcare environment. This method employed a robust steganographic technique to ensure the security of medical data within the network. This involved encrypting the patient's medical data through a hybrid cryptographic model, which combined the advanced encryption standard and blowfish algorithms. The encrypted medical data was then concealed within the patient's medical image, with the embedding points in the image determined using the Koblitz method. To embed the encrypted data, a hybrid elliptical curve cryptography approach was utilized. Subsequently, the image containing the embedded medical data underwent compression through a 5-level discrete wavelet transform. This comprehensive

process aimed to minimize storage requirements while simultaneously enhancing security and payload capacity within the system.

Refaee et al. [9] introduced an intelligent and secure Healthcare (HC) system called Fuzzy Dynamic Trust based Routing Protocol with Butter Ant Optimization Algorithm (FDT-RPL+BAOA) designed for an IoT platform. Initially, the data collected from IoT wearable sensors underwent preprocessing utilizing the k-nearest neighbor- based data imputation technique. Subsequently, a principal component analysis method was employed to reduce the higher dimensionality of the preprocessed data. The features derived from this processed data were extracted using a modified local binary pattern. Finally, a fuzzy dynamic trust-based routing protocol was developed, integrating an optimization technique to enhance security for IoT data. The findings demonstrated that this approach facilitated scalable and secure transmission of data within the IoT-HC system.

Arafat et al. [10] introduced the Distributed Energy efficient two-hop Clustering and Routing protocol (DECR) designed for wearable IoT devices, aiming to ensure consistent and dependable data communication. The protocol's initial step involved creating clusters by aggregating data from neighboring nodes within a two-hop range. Following this, Cluster Heads (CHs) were selected based on residual energy and node connectivity utilizing a modified grey wolf optimization algorithm. Additionally, an analytical model was devised to refine clusters, considering both inter- and intra-cluster transmission devices, to minimize transmission count and distance. Nevertheless, the protocol's drawback lies in its high computational complexity.

Sodhro et al. [11] introduced the adaptive Energy Efficient Algorithm (EEA), leveraging this effect during battery charging to improve energy efficiency, extend battery life, and increase throughput. Introducing novel algorithms could optimize the efficiency of smart healthcare systems by employing Machine Learning or Artificial Intelligence to reduce computational loads. Alazab, Lakshmanna, et al. [12] introduced the Modified Rider Optimization Algorithm (MROA) to choose Cluster Heads (CH) for IoT networks in smart cities. Additional measures such as Quality of Service (QoS), network traffic rate, and network density

will improve the performance of this approach. Rami Reddy, Ravi Chandra, et al. [13] introduced a method for selecting energy-efficient cluster heads using an Improved Grey Wolf Optimization (IGWO) approach. Broadening the applicability of this method to heterogeneous networks with increased node densities and a larger quantity of sensor nodes would further improve its efficiency.

3. RESEARCH PROBLEM

Due to the limited resources of IoT devices, challenges in energy, processing, computing, and storage resources pose significant hurdles in healthcare environments. Numerous studies aim to enhance network performance; nevertheless, achieving energy- efficient and secure data transmission in IoT-based healthcare systems remains unresolved. Some current methods transmit patient medical sensor data directly to the sink without employing clustering, impacting the network's Quality of Service (QoS) in terms of energy consumption, lifespan, packet loss ratio, and delay. While certain techniques adopt clustering-based data routing, efficient management of cluster data at the transmission gateway also influences QoS. Moreover, certain existing approaches lack security measures and reliable communication protocols for patient data transfer, rendering data vulnerable when transmitted through unsecured channels and susceptible to transmission errors that further impact network QoS. Existing methodologies still grapple with eliminating redundant and erroneous data generated by medical sensors, leading to increased energy consumption and bandwidth utilization in sensor nodes. Routing data through suboptimal paths or employing non-optimal multi-hop or single-hop communication in current mechanisms escalates energy consumption and diminishes packet delivery rates.

4. RESEARCH OBJECTIVES

The objectives of the research work are:

- To thwart unauthorized access and combat man-in-the-middle attacks, Double Hash Biometric-based Authentication (DHABA) is introduced.
- To diminish energy consumption and extend network longevity, Enhanced Mayfly Optimization Algorithm (EMOA) is introduced for cluster head selection.
- To ensure dependable and secure routing, Path Weighted Q Reinforcement

Learning (PWQRL) is suggested.

- To deal with the issues of slow convergence speed and the tendency of EMOA to fall into local optimum, EMOA with Active Elite Approach (EMOA-AEA) is proposed for cluster head selection.
- To handle quantum threats, Enhanced Binary Ring-Learning-with-Errors (EBRLWE) is proposed where an extra key is used for enhancing the healthcare data security.
- To handle complex state-action spaces, potentially accommodates diverse routing scenarios and optimizing decisions in a dynamically changing environment in IoT-based healthcare system, Deep Q Network (DQN) is introduced.

5. RESEARCH METHODOLOGY

5.1. Secure and Energy-Efficient Data Transmission Framework for IoT-based Healthcare Applications using EMCQLR AND EKECC

Data collected by IoT devices can be transmitted to medical professionals, granting doctors immediate access to their patient's information. However, the devices within the network face limitations in resources and computational power, leading to challenges in conserving energy. While clustering helps save energy in network nodes, current methods could be more efficient, addressing issues like increased energy consumption, uneven network load distribution, and heightened end-to-end delays. Additionally, ensuring the security and integrity of medical data has become a crucial concern in healthcare (HC) applications. A secure and energy-efficient framework is introduced for transmitting data in IoT-based healthcare (IoT-HC) systems using Enhanced Mayfly Clustering-Based Q Learner Routing (EMCQLR) and Exponential Key-based Elliptical Curve Cryptography (EKECC) techniques.

The proposed methodology follows a sequence of steps. Initially, Double Hash Biometric-based Authentication (DHABA) is employed for IoT user authorization, preventing unauthorized access to the healthcare network. Subsequently, the Enhanced Mayfly Optimization Algorithm (EMOA) selects the Cluster Head (CH) to organize clusters of IoT medical sensors and gather data from the nodes. Data routing to the

sink node includes a check for data duplication, facilitated by the Path-Weighted Q Reinforcement Learning (PWQRL) model. Finally, the EKECC algorithm encrypts data packets from the body sensors, ensuring the security of patient data during data transmission over unsecured wireless channels.

5.1.1 Proposed Work

A framework that ensures security and energy efficiency in IoT-HC applications has been developed using EMCQLR and EKECC. The method proposed comprises several stages: To commence, IoT user authorization is conducted through the DHBA approach. Subsequently, EMOA is employed for CH selection and the formation of clusters among IoT medical sensors. Following this, the patient's data

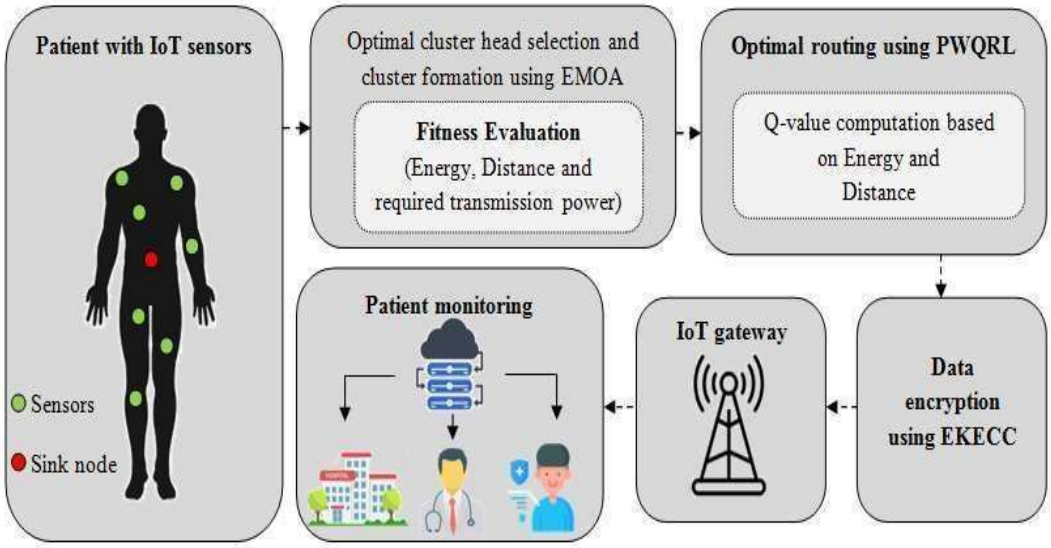

Figure 1: Schematic representation of Proposed Work

undergoes scrutiny using data deduplication principles. Upon identification and elimination of redundant data, the PWQRL technique is utilized to determine the most efficient data path. Finally, data acquired from the patient's sensors undergo encryption using the EKECC model. Each stage of this proposed model is elucidated below. The schematic representation of the entire proposed methodology is depicted in Figure 1.

5.1.2 Authentication

IoT serves numerous purposes, with both users and interconnected medical devices continually expanding. A man-in-the-middle (MIM) attack has the capability to identify monitored patients facing a healthcare emergency, manipulating

normal physiological data to prevent the system from triggering an alarm. This occurs when a hacker compromises communication between authorized

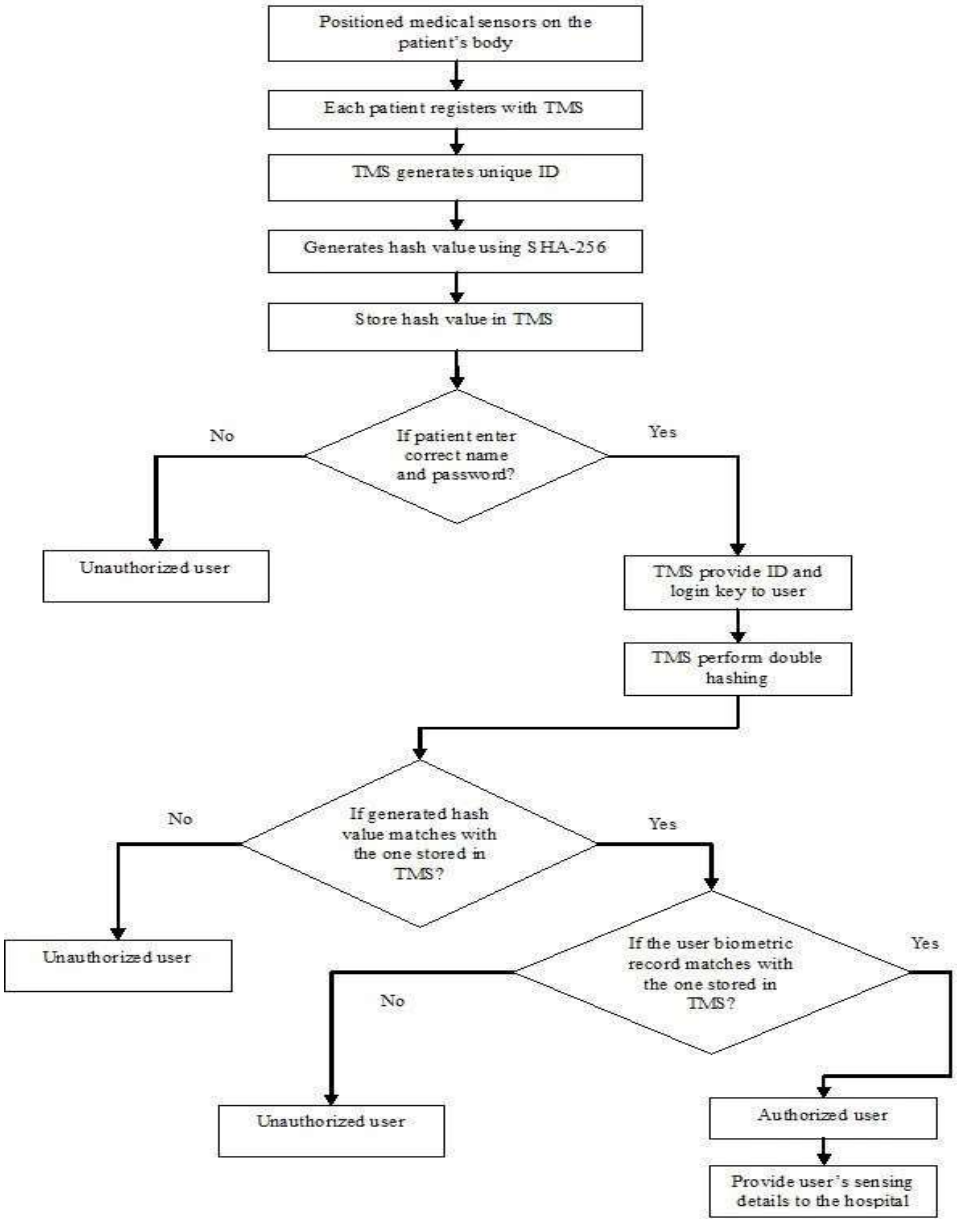
Positioned medical sensors on the patient's body
Each patient registers with TMS
TMS generates unique ID
Generates hash value using SHA-256
Store hash value in TMS
If patient enter correct name and password?
No
Yes
Unauthorized user
TMS provide ID and login key to user
TMS perform double hashing
If generated hash value matches with the one stored in TMS?
No
Yes
Unauthorized user
If the user biometric record matches with the one stored in TMS?
No
Yes
Unauthorized user
Authorized user
Provide user's sensing details to the hospital

Figure 2: Overall flow of Authentication Process

systems by inserting a malicious node or attacking the IoT network's communication protocols. Thus, safeguarding the IoT-HC network from unauthorized access and securely storing medical data on the cloud server is imperative. Data cannot be utilized against the network if attackers cannot access or interpret it. Implementing two-factor authentication (2FA) stands as the most effective measure to prevent interception of communications. This involves offering a second authentication layer

beyond password-based authentication.

5.1.3 Cluster Head Selection

Once patients receive authorization, their data is gathered via the CHs present in the network. The primary function of these CHs is to collect data from their respective cluster members and transmit it to the sink node. Clustering and CH selection operations are conducted to ensure an energy-efficient data transmission process in the IoT-HC network. In this proposed methodology, the optimal selection of CHs is achieved through the use of EMOA, considering fitness parameters like energy, distance, and transmission power.

Mayfly Optimization Algorithm (MOA) draws inspiration from the flight and mating behavior of adult mayflies and operates as a population-based metaheuristic method. It facilitates a random search while allowing the population to adapt based on the survival of the fittest. Each mayfly's position in the search area represents a potential solution to a problem. However, the conventional MOA exhibits limited global search capabilities in its initial stages and subsequently encounters slow convergence, often getting stuck in local optima. Moreover, there's a need for MOA and its variations to address higher-dimensional optimization challenges. This study presents two enhancements to tackle these limitations. Firstly, the implementation of Highly Disruptive Polynomial Mutation (HDPM) aims to elevate the quality of initial positions within the random population. Secondly, a novel adaptive inertia weight parameter is introduced to expedite convergence speed and accuracy, preventing the algorithm from getting trapped in local optimal solutions. These augmentations, termed EMOA, significantly enhance the traditional MOA's performance. Figure 3 shows the overall process of EMOA-based CH selection.

5.1.4 Cluster Formation and Data Deduplication

Following the CH selection process, the network is proceed with the formation of clusters through a series of steps. Firstly, the sink node initiates the process by broadcasting an ANNOUNCEMENT message to all nodes within the network. Upon receiving this broadcast from the sink node, nodes align themselves with the CH possessing the strongest received signal strength. Subsequently, the

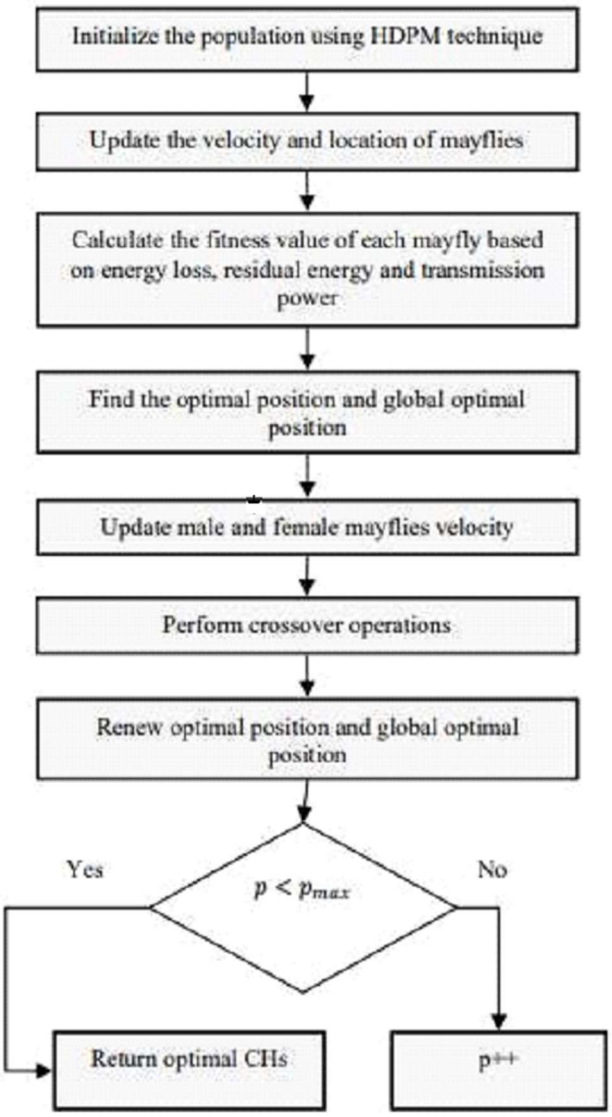
Initialize the population using HDPM technique
Update the velocity and location of mayflies
Calculate the fitness value of each mayfly based on energy loss, residual energy and transmission power
Find the optimal position and global optimal position
Update male and female mayflies velocity
Perform crossover operations
Renew optimal position and global optimal position
Yes
$p < p_{max}$
No
Return optimal CHs
p++

Figure 3: Overall flow of EMOA-based CH selection Process

Sensor Node (SN) forwards a request to join the cluster to the newly chosen CH. Finally, the CHs confirm the node's inclusion by accepting the cluster joining request, thereby establishing clusters within the network. This method orchestrates the formation of node clusters within the IoT-HC environment.

Upon cluster formation, data deduplication assesses the presence of duplicate content within patient data during each transmission phase. Elimination of duplicate content ensures that only the original data is retained, thereby conserving energy in nodes across each phase of data transmission. Upon sensing data, the SN conducts checks for redundancy within patient data. If redundancy is detected, the redundant data is withheld from transmission to the CH. Conversely, non-redundant data is

forwarded to the CH. The prevention of data redundancy involves referencing the data records table stored in the SN's network, thereby circumventing unnecessary redundancy in transmitted data.

In each transmission cycle, the SN stores the patient's sensed data in its onboard chip memory's data records table. Subsequently, during the initiation of each transmission phase, the node compares the current data value with previously stored data from prior transmission rounds in its chip memory. Identification of redundant data prompts the node to disregard it, omitting its transmission to the CH. Conversely, if no redundancy is detected, the node stores the data and proceeds to transmit it to the CH. This process ensures the conservation of energy and efficient transmission by filtering out redundant data at the node level before transmission.

5.1.5 Optimal Routing

Upon completing the redundancy check, the network undergoes routing, during which elected CHs transmit their cluster members' data to the sink. Within the proposed system, data forwarding or routing comprises two phases: direct and indirect. Direct forwarding entails sending data from SNs directly to the sink node if specific conditions are met:

1. When the SN is in close proximity to the sink (closer than it is to the CH).
2. When the SN has been designated as a CH.

If these criteria are not fulfilled by the SN, it then indirectly transfers its data to the sink through optimal forwarder nodes. Many existing methods choose routes for packet transmission randomly, resulting in decreased network longevity and increased energy consumption. In this scenario, optimal forwarder nodes are identified using a deep learning model, specifically the PWQRL technique. This model selects the most favorable routes for forwarding data from CHs to the sink by considering residual energy and the node-to-node distances. Nodes with higher path weights are deemed optimal forwarder nodes for efficient data routing. Figure 4 shows the overall process of PWQRL-based optimal routing.

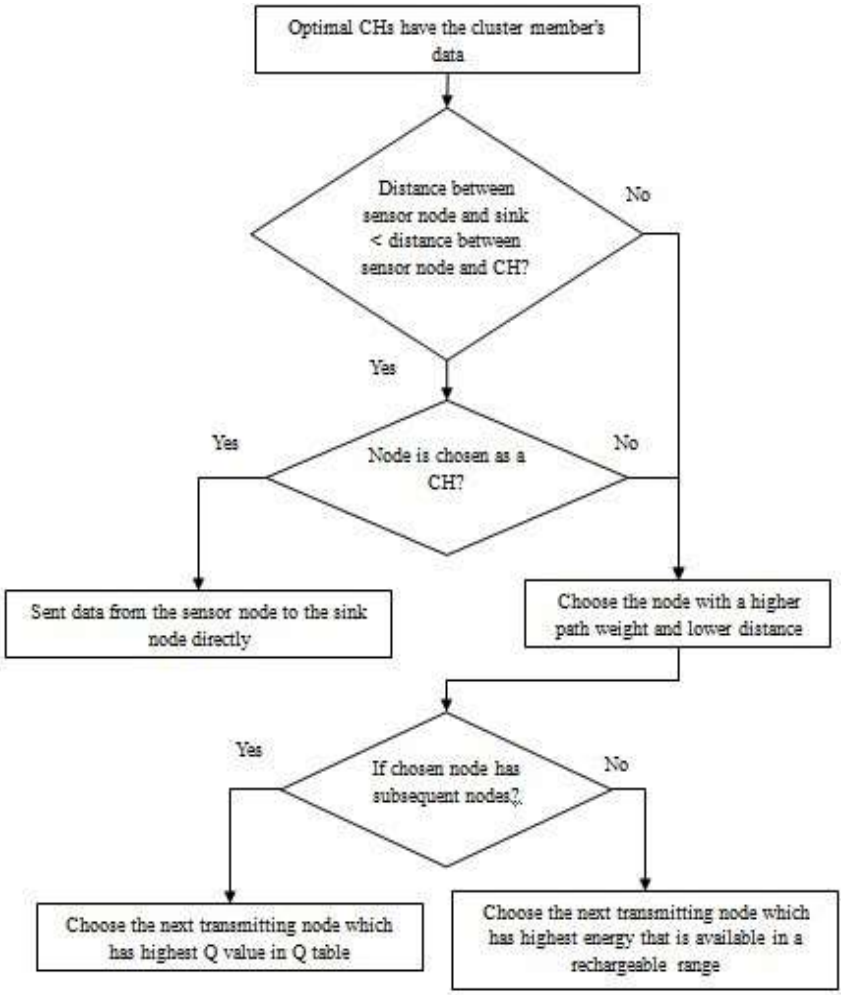
Optimal CHs have the cluster member's data
Distance between sensor node and sink < distance between sensor node and CH?
No
Yes
Yes
Node is chosen as a CH?
No
Sent data from the sensor node to the sink node directly
Choose the node with a higher path weight and lower distance
Yes
If chosen node has subsequent nodes?.
No
Choose the next transmitting node which has highest Q value in Q table
Choose the next transmitting node which has highest energy that is available in a rechargeable range

Figure 4: Overall flow of PWQRL-based optimal routing Process

5.1.6 Data Encryption

The selected optimal path undergoes DT to the TMS, wherein the patient's data are encrypted before transmission, ensuring heightened security over unsecured wireless channels. The encrypted patient data is received by the TMS, decrypted using the receiver's private key, and processed by hospital physicians to enhance patient services. This scheme achieves both security and efficiency for IoT-based healthcare systems, employing EKECC algorithms to encrypt data packets from body sensors.

Unlike the conventional ECC process that generates two keys for encryption and decryption, the proposed model introduces an additional key, the exponential key, enhancing cryptographic procedures. This key, derived during patient registration, modifies the private key generation process by being concatenated or added to it.

Employing this exponential key in encryption and decryption operations within ECC fortifies the security against potential attackers during data transmission. This approach, termed EKECC, strengthens data security and thwarts potential attacks during DT, ensuring a higher level of protection for healthcare data.

5.2 Enhanced Mayfly Optimization with Active Elite Approach Based Cluster Head Selection for Energy Efficient IoT based Healthcare Monitoring System

EMOA encounters a local optimum issue, exacerbated by the exponential growth in the healthcare data volume, leading to challenges in selecting an optimal CH despite extensive search efforts. To address this, the EMOA-Active Elite Approach (EMOA- AEA) is introduced, aiming to overcome suboptimal CH selection scenarios. Within each EMOA-AEA cycle, the algorithm identifies the best mayfly based on objective functions and dynamically adjusts its search radius. Additionally, multiple elite mayflies are generated within the search area. If these newly produced elites surpass the current best one in CH selection, they replace it, thereby enhancing the global search capability of EMOA for better CH selection. This advancement not only improves the algorithm's efficacy in choosing superior CH but also fosters an energy-efficient environment for IoT-HC monitoring systems.

5.2.1 Proposed Method

Authorized patients' data is gathered through CHs within the network in an IoT-HC system. CH selection is crucial for network management, ensuring reliable communication, and optimizing resource usage. A CH, serving as a designated node, coordinates communication and data exchange among clustered nodes. Its selection significantly influences IoT-HC system management, resource optimization, data security, and energy efficiency, ultimately impacting patient outcomes and care quality. EMOA-AEA, based on multiple objectives like transmission power, energy, and distance, facilitates optimal CH selection. EMOA utilizes an adaptive inertia weight to expedite convergence speed and accuracy, preventing local optima; however, its effectiveness is limited due to user-specified adaptive weight criteria. Therefore, an AEA within EMOA is implemented to further enhance convergence speed and accuracy. Figure 5 shows the overall flow of CH selection based on EMOA-AEA.

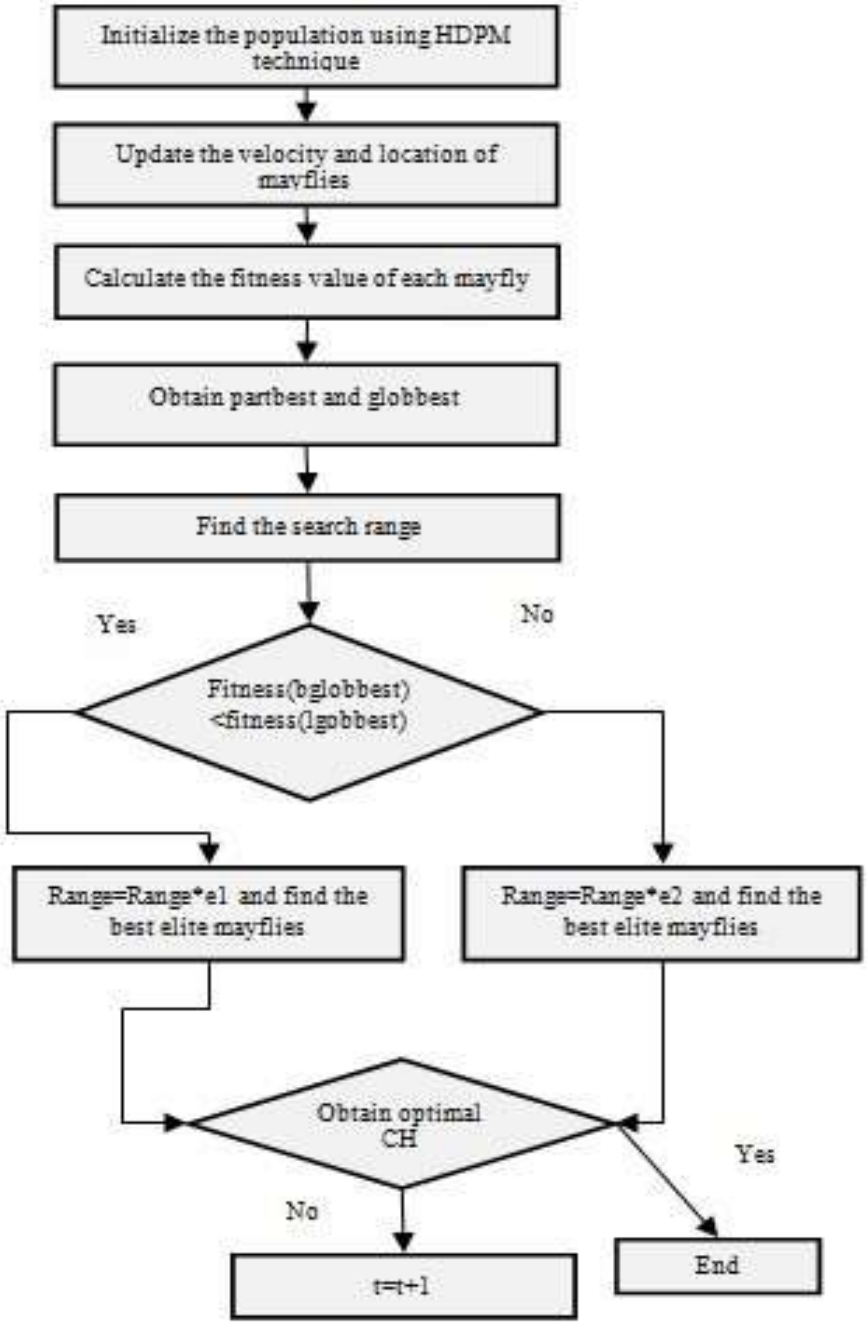

Figure 5: Overall flow of EMOA-AEA based CH selection Process

5.2.2 Encryption and Routing

Upon identifying the best CHs through EMOA-AEA, nodes in the IoT-HC system are clustered. Subsequently, redundant data packets are identified and disregarded by the nodes, preventing their transmission to the CH. Following this process, PWQRL technique is utilized to establish efficient routes for data transmission from CH to sink nodes within the network. Once the optimal paths are

chosen, the EKECC algorithm is applied to encrypt data packets originating from body sensors, ensuring enhanced security for patient data during transmission over unsecured wireless channels.

5.3 Enhanced Mayfly with Active Elite Approach Clustering based Deep Q Learner Routing with BRLWE for IoT-based Healthcare Monitoring System

EMOA Enhanced Mayfly with Active elite approach Clustering based Deep Q Learner Routing with Enhanced Binary ring-learning-with-errors (EMACDQLEB) is proposed for secure and energy-efficient IoT-HC system. EMACDQLEB integrates an Enhanced Binary Ring-Learning-with-Errors (EBRLWE) approach, diverging from Exponential Key-based Elliptical Curve Cryptography (EKECC), to fortify the security of patient data in IoT-based Healthcare (HC) systems. EBRLWE ensures resistance against emerging quantum threats, contrasting with EKECC's vulnerability to quantum attacks, making it a more viable long-term security solution. Additionally, to further enhance data security, EMACDQLEB incorporates an additional key generated through a hash function applied to the login key within EBRLWE. For routing within IoT-based HC systems, EMACDQLEB adopts Deep Q-Networks (DQN) over Path-Weighted Q Reinforcement Learning (PWQRL). DQN's adaptability in managing complex state-action spaces enables it to address various routing scenarios effectively, optimizing decisions in the dynamic IoT-based HC environment.

5.3.1 Proposed Work

Securing the IoT-HC network and safeguarding medical data in the cloud server is essential due to the increasing number of users and connected medical devices. To achieve this, an authentication scheme is necessary for network protection. Upon initializing sensors within a patient's body, DHBA [6] is used in an enhanced secure and energy-efficient data transmission system for authentication. Following authentication, authorized patient data is gathered through the CH within the network. The CH collects data from its cluster members and forwards it to the sink node. EMOA-AEA is utilized for clustering and CH selection processes. Upon CH selection, announcement messages are sent to all nodes to form clusters within the network.

Once clusters are established, the identification of redundant or duplicate data occurs to conserve nodes' energy during data transmission. The sink node's data records table is referenced for this purpose. Any identified duplicate data is ignored by the node and not transmitted to the CH.

5.3.2 Deep Q Network-based Routing Process

DQN, a successful reinforcement learning method, is applied in routing, determining the best path for data packets from CHs to sink nodes in a network. Its algorithm learns and adjusts to network changes, employing a neural network to estimate the Q-function. This function, evaluating actions in states, gets updated by exploring the network for experience and exploiting it to enhance its learning.

5.3.3 Data Encryption using EBRLWE

EBRLWE encryption involves a secret key and a public key, where the secret key is a concise binary vector, while the public key comprises a matrix derived from a specific distribution. To heighten data security, an additional key is introduced during BRLWE's cryptographic process. In EBRLWE, the secret key is created by concatenating a hash value obtained during registration. This additional key is incorporated during encryption and removed during decryption. To encrypt a patient's data, it's initially converted into a binary vector, then multiplied by the public key matrix with a slight addition of noise. The resulting cipher text is transmitted to the TMS. Decryption of the cipher text involves the TMS utilizing the secret key and the hash value of the login key created during registration to perform a dot product with the cipher text. This produces a noisy rendition of the original data, which can be decoded to recover the patient's information. Finally, the encrypted data is send from CH to the sink node through the optimal route which is selected DQN.

6. THESIS ORGANIZATION

Chapter 1 – *"Introduction "*presents the IoT, IoT-HC system and risk factors in IoT-HC system. We discuss the need of security, optimal routing for data transmission and clustering of nodes in IoT-HC system. We also outline the techniques used for security, optimal routing and clustering of nodes in IoT-HC system.

Chapter 2 *"Literature Review"* provides comprehensive survey of different existing techniques used for security, optimal routing and clustering of nodes in IoT-HC system.

Chapter 3 *"Secure and Energy-Efficient Data Transmission Framework for IoT-based Healthcare Applications using EMCQLR and EKECC" proposed* for securing and transmitting data in energy-efficient manner in IoT-HC systems.

Chapter 4 *"Enhanced Mayfly Optimization with Active Elite Approach Based Cluster Head Selection for Energy Efficient IoT based Healthcare Monitoring System"* proposed to deal with the issues of slow convergence speed and the tendency of EMOA to fall into local optimum. establishes a definite area around the most optimal mayfly in the present population, which is used to identify the top-performing CH.

Chapter 5 "*Enhanced Mayfly with Active Elite Approach Clustering based Deep Q Learner Routing with EBRLWE for IoT-based Healthcare Monitoring System"* proposed to safeguard patient data due to EBRLWE offers quantum-resistant security against emerging quantum threats, making it a suitable choice for securing IoT-based HC systems. Moreover, DQN is employed for routing which handles complex state- action spaces, potentially accommodating diverse routing scenarios and optimizing decisions in a dynamically changing environment in IoT-based HC system.

Chapter 6 *"Conclusion and Future work"* summarizes the key results, conclusions of this thesis and outlines the future scope of work.

7. REFERENCES

1. Haghi, M., Neubert, S., Geissler, A., Fleischer, H., Stoll, N., Stoll, R., Thurow, K., A flexible and pervasive IoT-based healthcare platform for physiological and environmental parameters monitoring., *IEEE Internet of Things Journal*, **7**(6)(2020), 5628-5647.

2. Domínguez-Bolaño, T., Campos, O., Barral, V., Escudero, C.J., García-aya, J.A., An overview of IoT architectures, technologies, and existing open-source projects., *Internet of Things*, **100626**(2022).

3. Rejeb, A., Rejeb, K., Treiblmaier, H., Appolloni, A., Alghamdi, S., Alhasawi, Y., Iranmanesh, M., The Internet of Things (IoT) in Healthcare: Taking Stock and Moving Forward., *Internet of Things*, **100721(**2023**)**.

4. Shahraki, A., Taherkordi, A., Haugen, Eliassen, F., A survey and future directions on clustering: From WSNs to IoT and modern networking paradigms., *IEEE Transactions on Network and Service Management*, **18**(2)(2020), 2242- 2274.

5. Kaur, N., Sood, S.K., An energy-efficient architecture for the Internet of Things (IoT)., *IEEE Systems Journal*, **11**(2)(2015), 796-805.

6. Selvaraj, S., Sundaravaradhan, S., Challenges and opportunities in IoT healthcare systems: a systematic review., *SN Applied Sciences*, **2**(1) (2020), 1-8.

7. Almalki, F.A., Soufiene, B.O., EPPDA: an efficient and privacy-preserving data aggregation scheme with authentication and authorization for IoT-based healthcare applications., *Wireless Communications and Mobile Computing*, **2021**(1) (2021).

8. Prasanalakshmi, B., Murugan, K., Srinivasan, K., Shridevi, S., Shamsudheen, S., Hu, Y.C., Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography., *The Journal of Supercomputing*, **78**(1) (2022), 361-378.

9. Refaee, E., Parveen, S., Begum, K.M.J., Parveen, F., Raja, M.C., Gupta, S.K.,Krishnan, S., Secure and scalable healthcare data transmission in IoT based on optimized routing protocols for mobile computing applications., *WirelessCommunications and Mobile Computing*, **2022**(1) (2022), 1-12.

10. Arafat, M.Y., Pan, S., Bak, E., Distributed Energy-Efficient Clustering and Routing for Wearable IoT Enabled Wireless Body Area Networks., *IEEE Access,* **11**(2023), 5047-5061.

11. Sodhro, A.H., Al-Rakhami, M.S., Wang, L., Magsi, H., Zahid, N., Pirbhulal, S., Ahmad, A., Decentralized energy efficient model for data transmission in IoT- based healthcare system., *IEEE 93rd Vehicular Technology Conference (VTC2021-Spring),* (2021), 1-5.

12. Alazab, M., Lakshmanna, K., Reddy, T., Pham, Q.V., Maddikunta, P.K.R., Multi- objective cluster head selection using fitness averaged rider optimization algorithm for IoT networks in smart cities., *Sustainable Energy Technologies and Assessments*, **43**(2021), 100973.

13. Rami Reddy, M., Ravi Chandra, M.L., Venkatramana, P., Dilli, R., Energy-efficient cluster head selection in wireless sensor networks using an improved grey wolf optimization algorithm., *Computers*, **12**(2)(2023), 35.

8. LIST OF PUBLICATIONS

Journal of Publications –SCI

1. Balakrishnan, D., T. Dhiliphan Rajkumar, S. Dhanasekaran, and B. S. Murugan. "Secure and energy-efficient data transmission framework for IoT-based healthcare applications using EMCQLR and EKECC." *Cluster Computing* **27**(3) (2024): 2999-3016.

2. Balakrishnan, D., and T. Dhiliphan Rajkumar. "Enhanced mayfly with active elite approach clustering based deep Q learner routing with EBRLWE for IoT-based healthcare monitoring system." *Multimedia Tools and Applications* (2024): 1-24.

Journal of Publications –SCOPUS

3. Balakrishnan, D., and T. Dhiliphan Rajkumar, "Enhanced Mayfly Optimization with Active Elite Approach Based Cluster Head Selection for Energy Efficient IoT based Healthcare Monitoring System." In *2023 2nd International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN)*, IEEE, (2023), 1-6.